Notice of Allowability	Application No.	Applicant(s)	
	09/928,704	SOLINAS, JEROME ANTHONY	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Terminal Disclaimer filed January 24, 2005*.

2. ☒ The allowed claim(s) is/are *1*.

3. ☒ The drawings filed on *included by Examiner's Admendment* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *herein included* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

E. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

Allowable Subject Matter

Claim 1 are allowed.

The following is an examiner's statement of reasons for allowance:

As per claim 1, the prior art of record does not teach or suggest a combination as claimed, in which the modulus p is selected from the group of equations as specified in step (a), to be utilized in the method for exchanging a cryptographic key between two users, described in steps (b) through (l). The prior art described in page 6 of applicant's *Background of the Invention* discloses the use of a class of numbers in the form of 2^q-C chosen to create a more efficient modular reduction, to be utilized in a method for identifying users. At the time of the invention, there would be no motivation for a person of ordinary skill in the art to use the applicant's combination. Therefore, claim 1 is allowable.

Interview Summary

Please refer to the Examiner's "Annotated Marked-Up Drawings" included as page 2 of this office action for changes made to Figure 1 as per Attorney's request.

"ANNOTATED MARKED-UP DRAWING"

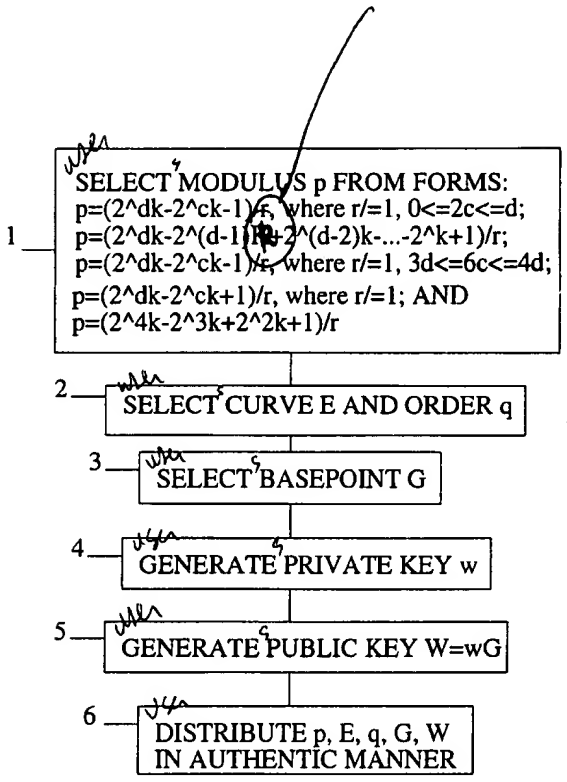

FIG. 1

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Attorney Robert D. Morelli on August 5, 2005.

Please amend Claims in accordance with Examiner's "Claim Amendments" included as pages 4-5 of this office action.

Please amend Specifications in accordance with Examiner's "Specification Amendments" included as pages 6-11 of this office action.

The following changes to the drawings have been approved by the examiner and agreed upon by applicant: Please replace Figure 1 with Examiner's "Replacement Sheet" Figure 1 as included in page 12 of this office action.

CLAIM AMENDMENTS

Claim 1 (currently amended): A method of exchanging a cryptographic key between two users, comprising the steps of:

a) each of said two users selecting a value p from the group of equations consisting of:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where r /= is not equal 1, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where d is even, and where k is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where r /= is not equal 1, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r;$$

b) each of said two users selecting an elliptic curve E and an order q;

c) each of said two users selecting a basepoint $G=(G_x, G_y)$ on the elliptic curve E, where G is of order q ;

d) each of said two users generating a private key w, where w is an integer;

e) each of said two users generating a public key $W=wG$, where W is the corresponding user's public key, where w is the corresponding user's private key, and where G is the corresponding user's basepoint ;

f) each of said two users distributing their p, E, q, G, and W in an authentic manner;

g) the two users agreeing on p, E, q, G, W_1, and W_2, where W_1 is the public key of one of said two users, and where W_2 is the public key of the other of said users;

h) each of said two users generating a private integer;

i) each of said two users multiplying G by each of said user's private ineteger generated in the last step using a form of p agreed upon;

j) each of said two users transmitting the result of the last step to the other of said two users;

k) each of said two users combining one of said two user's private integer and public key with the other of said two user's result of step (j) and public key using the form of p agreed upon to form a common secret point between each of said two users; and

l) each of said two users deriving the cryptographic key from the common secret point.

SPECIFICATION AMENDMENTS

(Replace the third full paragraph on page 2 with the following paragraph.)

The use of cryptographic key pairs was disclosed in U.S. Pat. No. 4,200,770, entitled "CRYPTOGRAPHIC APPARATUS AND METHOD." U.S. Pat. No. 4,200,770 also disclosed the application of key pairs to the problem of key agreement over an insecure communication channel. The algorithms specified in this U.S. Pat. No. ~~4,200,700~~ 4,200,770 rely for their security on the difficulty of the mathematical problem of finding a discrete logarithm. U.S. Pat. No. 4,200,770 is hereby incorporated by reference into the specification of the present invention.

(Replace the third full paragraph on page 7 with the following paragraph.)

It is another object of the present invention to securely exchange a cryptographic key between two users over a public channel based on the discrete logarithm problem and using a modulus *p* of the form selected from the following forms:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where *r* /= is not equal to 1, and where *GCD(c,d)*=1, where *GCD* is a function that returns the greatest common denominator of the variables in parenthesis;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where *d* is even, and where *k* is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where r /= is not equal to 1, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r.$$

(Replace the first full paragraph on page 8 with the following paragraph.)

The present invention is a method of performing a cryptographic key exchange on an elliptic curve in an efficient manner (i.e., in fewer steps than the prior art), using a modulus p in a form selected from the following forms:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where r /= is not equal to 1, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where *d* is even, and where *k* is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where *GCD(c,d)*=1;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where *r* /= is not equal to 1, and where *GCD(c,d)*=1; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r.$$

(Replace the third full paragraph on page 9 with the following paragraph.)

The first step is selecting a value *p* from the group of equations as follows:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where *r* /= is not equal to 1, and where *GCD(c,d)*=1;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where *d* is even, and where *k* is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where r != is not equal to 1, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r.$$

(Replace the last paragraph on page 11 with the following paragraph.)

The present invention is a method of performing a cryptographc key exchange on an elliptic curve in an efficient manner (i.e., in fewer steps than the prior art), using a modulus p in the form selected from the following forms:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where r != is not equal 1, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where d is even, and where k is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where r != is not equal 1, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r.$$

(Replace the last paragraph on page 13 with the following paragraph.)

Figure 1 is a list of steps for selecting parameters that each user must do. The first step 1 of the present method is for a user to select a modulus p from the group of equations as follows:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where r != is not equal 1, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where d is even, and where k is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where $r \neq$ is not equal 1, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r.$$

"REPLACEMENT SHEET"

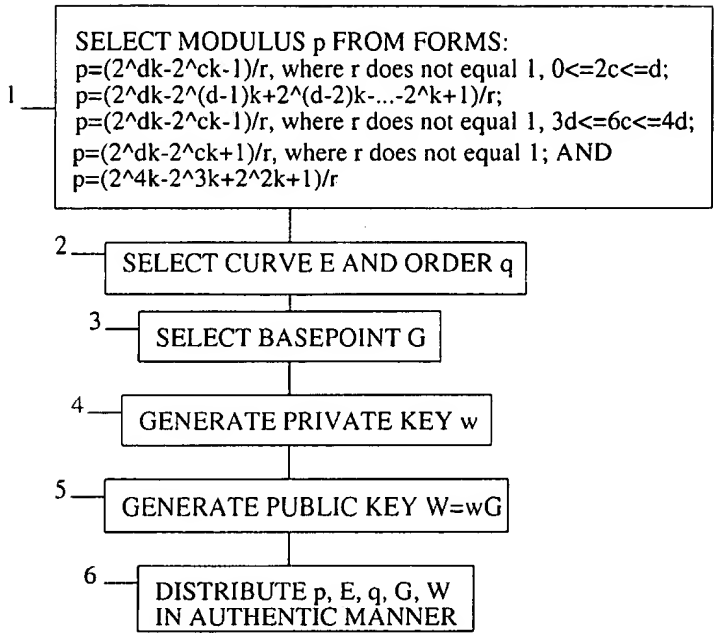

FIG. 1

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T. Teslovich
August 4, 2005

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER